Amendments to the Specification:

Please amend the specification as follows:

Please replace paragraph number [0008] with the following rewritten paragraph:

One advantage of using a separate unit, when establishing a secure connection, is that it will be much easier to re-establish a connection to the data communication apparatus. Thus, it is possible to save information, for example signatures, secret keys, etc., in the memory means, and the information may be re-used in another secure connection. In order to avoid fraud, the re-use of a secure connection can be restricted for limited period of time. By saving this information in the memory means the second object will be achieved.

Please replace paragraph number [0048] with the following rewritten paragraph:

To establish a secure connection, the client 1 connects to the separate unit, accessing the wireless communication network 50 connected to the server 20. Then the client 1 transmits an encrypted request 60 through the gateway 30. The encrypted request 60 comprises information of which pre-defined algorithm(s) the client 1 supports. When the gateway 30 receives this decrypted request 60, it sends 70 the encrypted request to the origin server 40. The origin server 40 chooses at least one algorithm, associated with a public key and a private key, and transmits a message 80 back to the gateway 30. The gateway encrypts the message and sends it 90 to the client 1. This message 90 comprises the public key information about which algorithm the server 20 has chosen. When the client 1 receives the encrypted message 90, comprising the public key, it will generate a master secret code, and calculates a signature based on the chosen algorithm, the public key and the master secret code. Thereafter, the client 1 will transmit an encrypted response 65 to the gateway 30. This encrypted response 65 comprises the calculated signature. When the gateway 30 receives the encrypted response [[80]] 65, comprising the signature, it will decrypt the response 75 and send it to the origin server 40. The origin server 40 will calculate the master secret code based on the chosen algorithm, the signature received, and its private key. Finally, the origin server 40 sends a final message 85 to the client through the gateway 30. If the origin server 40 has accepted the client [[1]] request 60, the server will be able to establish a secure

connection between the origin server 40 and the client 1, else the connection will be terminated.

Please replace paragraph number [0054] with the following rewritten paragraph:

The server 20 will furthermore transmit a server certificate message 102. The server certificate message 102 will always immediately follow the server hello message 101, and the purpose of this server certificate message 102 is to identify the ~~encryptation~~ encryption algorithm selected by the server from the key exchange list included in the client hello message 100. The server certificate message 102 will include a so-called certificate carrying a public key for the selected encryption algorithm. The server certificate message 102 includes information about the issuer of the certificate, the beginning and the end of the validity period, and parameters relevant or the public key. The server controls the validity period and, when the granted validity period is expired, the client has to renew the secure connection. The length of the validity period will typically be in the level of a week or more. The maximum number of session will also have to be identified.